VIA ELECTRONIC FILING

Marlene H. Dortch
Secretary, Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Commercial Availability of Navigation Devices, MB Docket No. 16-42, CS Docket No. 97-80

Dear Ms. Dortch:

On July 6, 2016 the undersigned, on behalf of Beyond Broadband Technology, LLC (BBT) met with Gigi Sohn, Counselor to the Chairman, Scott Jordan, Chief Technologist, and Eric Feigenbaum, Director of Outreach & Strategy of the Commission's staff to discuss the above-referenced dockets.

Discussion centered on one particular detail of current considerations surrounding the "app" approach to satisfying the Commission's objective of establishing new rules for MVPD set top boxes. In published reports and filings regarding that approach the suggestion has been made that the core IP mechanism for implementation would be HTML5. BBT agrees and supports that approach. We wanted to reiterate, however, as we have done throughout these proceedings and during the DSTAC deliberations prior to them, that any approach dealing with transmission, encryption, security and privacy should anticipate and include the ability to use both software and hardware technology solutions. As the Commission knows, BBT has developed a downloadable security technology currently in use. We believe it, or technology like it, will ultimately be found to be far more secure than any software approach. It can also offer far more individualized control and be more responsive to any attack than current software designs.

The problem we highlighted in this discussion was that the current software HTML5 CDM (content decryption module) or security module approach suffers from the same potential risk for both distributors and consumers; should the underlying software be breached, there is no effective way to "repair" it. Content owners would effectively either be forced to send their product essentially "in the clear" or withhold their high value product from IP distribution. Just changing encryption parameters would not solve the underlying breach. Consumers would be left with equipment that was effectively neutered. Hardware-based security solutions such as BBT's are designed to be both nimble and repairable, thus protecting both consumers and data providers.

We explained that the HTML5 security structure already includes a CDM or security module that anticipates and allows for the use of either software or hardware security. We made it clear that we are not asking the Commission to select any particular security approach. Rather we just want to make sure that any structure ultimately chosen continues to have the flexibility to implement either a software or hardware solution.

We noted that while there appears to be current acceptance of the limitations of software (DRM) security, as IP broadband distribution becomes more ubiquitous the result will be that those software solutions will be put under ever-increasing stress and attack because of the ballooning threat target they are trying to protect. It is foreseeable that it will ultimately burst. Meanwhile, hardware security approaches such as BBT's can limit the threat target, effectively, to one device should that be desired, regardless of how many have been deployed.

As we explained, at some point we believe encryption experts and the entities involved in both creating and distributing digital data and entertainment products will recognize that a hardware security solution, whether already built in to consumer devices or capable of being added to them (such as through the use of a USB dongle) will represent the only effective way to protect content and privacy (for entertainment viewers as well as for any other data they may choose to access, such as private health care records and the like.) The higher the value of the product being distributed, or the more secure the data needs to be, will, we suggested, ultimately result in the need to protect that material with hardware solutions, not software which will be under constant successful attack, as it is today.

Again, we made it clear that we are not seeking any special designation or selection by the Commission. However, should it move forward with either the "app" approach, which we support, or the original NPRM effort to design new hardware technology, which we believe, and have stated before, would likely be far too complicated to be useful or effective, either should specifically retain the flexibility to accommodate and implement both software and hardware security solutions. We noted that it is hard to see how any of the parties would find this objectionable.

Please direct any questions to the undersigned.

Sincerely,

/s/ Stephen R. Effros
Director, Strategic Planning and Communications
Beyond Broadband Technology, LLC (BBT)
PO Box 8
Clifton, VA 20124
703-631-2099
steve@effros.com

Cc:
Gigi Sohn
Scott Jordan
Eric Feigenbaum